

 Georgia Technology Authority	Georgia Technology Authority	
Title:	System Operations Documentation	
PSG Number:	SS-08-027.01	Topical Area: Security
Document Type:	Standard	Pages: 2
Issue Date:	3/31/08	Effective Date: 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Requires agencies to document system operational procedures.	

PURPOSE

This standard establishes a requirement that system owners maintain system documentation and standard operating procedures.

To adequately protect state information resources and facilities, personnel must understand their roles, responsibilities and how to perform them.

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency during system transition to operations and to maintaining the security support structure. System documentation and formalizing operational procedures with sufficient detail helps to eliminate security incidents and oversights, gives new personnel sufficiently detailed instructions and provides a quality assurance function to help ensure that system operations will be performed correctly and efficiently.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

All phases of the systems lifecycle shall have supporting documentation.

System owners shall formally document, approve and maintain detailed system and security operations and maintenance manuals/procedures for day-to-day and emergency IT operations.

System Owners shall ensure that documentation is current and personnel know where to find and how to reference them.

Operational documentation containing sensitive information shall be assigned an appropriate security categorization and protected from unauthorized access and

Title:	System and Security Operations Documentation
--------	--

disclosure.

Operations and maintenance documentation shall include, where applicable:

- System and communications build/configuration specifications
- Documented authorization from senior management official to operate the system
- System administration/maintenance manuals
- Security Plans
- Security operations policy and procedures for:
 - Access Management
 - Data center security and safety
 - Incident Response and Handling
 - Baseline security configurations (OS, hardware/software, network, applications)
- Service Level Agreements
- Back-ups, storage and restore procedures
- Virus Update and Patch Management procedures
- Information, data, equipment and media handling, processing and disposal procedures
- Business Continuity, Contingency, Disaster response and recovery plans
- Change Management procedures

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Systems and Development Lifecycle (Policy)
- System Security Plans (Standard)
- System Implementation and Acceptance (Standard)

REFERENCES

- NIST SP800-64 Security Considerations for the Systems Development Lifecycle
- NIST SP800-100 Information Security Handbook for Managers

Note: The PSG number was changed from S-08-027.01 on September 1, 2008.

Effective Date:	March 31, 2008	2 of 2
-----------------	----------------	--------